The Corner Surgery
Southport

117 Fylde Road
Southport, PR9 9XP
Tel: 01704 506055
Fax: 0151 247 6238
Email: gp.n84613@nhs.net

Data Protection Impact Assessment (DPIA) Policy

Summary

- *Prepared by* Dr David Smith (Data Protection Officer)
- *Effective from* 25th May 2018
- *Last reviewed* 29th March 2023
- *Next review date* 31st March 2024

Introduction

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

The General Data Protection Regulation (GDPR) introduces a new obligation to do a Data Protection Impact Assessment (DPIA) before carrying out types of processing likely to result in a high risk to individuals' interests.

A DPIA does not have to eradicate the risks altogether but should help to minimise risks and assess whether or not remaining risks are justified.

DPIAs are part of The Corner Surgery's (hereby referred to as "we", "us" or "the practice") accountability obligations under the GDPR, and an integral part of the 'data protection by default and by design' approach. DPIAs reflect the more risk-based approach to data protection obligations taken throughout the GDPR.

An effective DPIA will help us to:

- Identify and fix problems at an early stage
- Identify and minimise privacy risks associated with new projects
- Demonstrate compliance with our data protection obligations
- Meet individuals' expectations of privacy
- Help avoid reputational damage which might otherwise occur.

An effective DPIA can also bring broader compliance, financial and reputational benefits, help us demonstrate accountability, and build trust and engagement with patients.

Privacy impact assessments (PIAs) have been used for many years as a good practice measure to identify and minimise privacy risks associated with new projects.

The Information Commissioner's Office (ICO) does not expect us to do a new DPIA for existing processing where we have already considered relevant risks and safeguards

(whether as part of a PIA or another formal or informal risk assessment process) - *unless there has been a significant change to the nature, scope, context or purposes of the processing since that previous assessment*.

We will, therefore, monitor all existing data sharing and processing and must consider the need for a DPIA should there be any such changes.

DPIAs are also relevant if we are planning to make *changes* to an existing system/ project/ data sharing/ processing. If we make any significant changes to how or why we process personal data, or to the amount of data we collect, then we will need to show that our DPIA assesses any new risks.

A DPIA should also be performed, or reviewed, if there is an external change to the wider context of the processing, e.g. a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing we do or the vulnerability of a particular group of Data Subjects.

When Must We Do a DPIA?

We must do a DPIA where a type of processing is *likely to result in a high risk* to the rights and freedoms of individuals – *Article 35(1)*.

To assess whether something is 'high risk', the GDPR is clear that we need to consider both the likelihood and severity of any potential harm to individuals:

- 'Risk' implies a more than remote chance of some harm
- 'High risk' implies a higher threshold, either because the potential harm is more likely, or because it is more severe, or a combination of the two.

Assessing the likelihood of risk is, in that sense, part of the job of a DPIA. The starting point is to ask ourselves "are there features about the processing that point to the *potential* for high risk"? We are screening for any red flags that indicate that we need to do a DPIA to look at the risk (including the likelihood and severity of potential harm) in more detail.

Article 35(3) sets out three types of processing which always require a DPIA:

Systematic and Extensive Profiling with Significant Effects

The term 'extensive' implies that the processing also covers a large area, involves a wide range of data or affects a large number of individuals. A 'significant effect' is something that has a noticeable impact on an individual and can affect their circumstances, behaviour or choices in a significant way. This might include something that affects a person's financial status, health, reputation, access to services, or other economic or social opportunities.

Large Scale Use of Sensitive 'Special Category' Data

To decide whether or not processing is on a large scale, we should consider:

- The number of individuals concerned
- The volume of data
- The variety of data
- The duration of the processing
- The geographical extent of the processing.

Public Monitoring

The Article 29 working party of EU data protection authorities has published guidelines with nine criteria, which may act as indicators of likely high risk processing, of which those in italics are relevant to general medical practice:

- *Evaluation or scoring (e.g. profiling)*
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- *Sensitive data or data of a highly personal nature*
- Data processed on a large scale
- *Matching or combining datasets*
- *Data concerning vulnerable Data Subjects*
- Innovative use or applying new technological or organisational solutions
- Preventing Data Subjects from exercising a right or using a service or contract.

The Corner Surgery is a small practice, with ~4000 Data Subjects and ~15 staff, so most processing will not be on a large scale.

The ICO details a further ten types of processing that automatically require a DPIA:

- *New Technologies:* processing involving the use of new technologies or the novel application of existing technologies (including artificial intelligence)
- *Denial of Service:* decisions about an individual's access to a product, service, opportunity or benefit, which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data
- *Large-Scale Profiling:* any profiling of individuals on a large scale
- *Biometrics:* any processing of biometric data
- *Genetic Data:* any processing of genetic data, other than that processed by an individual GP or health professional for the provision of health care direct to the Data Subject
- *Data Matching:* combining, comparing or matching personal data obtained from multiple sources
- *Invisible Processing:* processing of personal data that has not been obtained direct from the Data Subject, in circumstances where the controller considers compliance with Article 14 would prove impossible or involve disproportionate effort
- *Tracking:* processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment
- *Targeting of Children or Other Vulnerable Individuals:* the use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children
- *Risk of Physical Harm:* where the processing is of such a nature that a personal data breach could jeopardise the [physical] health or safety of individuals.

Advice of the Data Protection Officer (DPO)

The DPIA is the responsibility of the data controller, in this case, The Corner Surgery.

The DPO, currently Dr David Smith, will provide advice on:

- Whether we need to do a DPIA

- How we should do a DPIA
- Whether to outsource the DPIA or do it in-house
- Whether it is appropriate for a group of Data Controllers to perform a joint DPIA
- Whether we need or require the assistance of any Data Processor in performing the DPIA
- Whether we should, or need to, consult with individuals and other stakeholders
- What measures and safeguards we can take to mitigate risks
- Whether we have done the DPIA correctly
- The outcome of the DPIA and whether the processing should go ahead.

The practice will record the DPO's advice on the DPIA. If the practice does not follow his advice, it will record the reasons and ensure that it can justify that decision. If the practice decides not to do a DPIA, then we will document that decision and the reasons for it, including the DPO's advice. If the practice is in any doubt, the advice of the ICO is that they "*strongly recommend you do a DPIA*".

Performing a DPIA

A DPIA may cover a single processing operation or a group of similar processing operations.

The Information Governance (IG) Lead and DPO, Dr David Smith, will be responsible for carrying out any DPIA, and will present the report at a partnership meeting. The DPIA will not make a recommendation as to whether to proceed with the processing; rather the options available (including whether processing would be manifestly unlawful) should the practice choose to proceed with any such data sharing project.

All partners who do not have a conflict of interest in the processing are entitled to vote on whether to permit the processing and under what conditions. The IG Lead and DPO is not (and cannot be) solely responsible for that decision; it is for *the partnership as a whole* to decide. If the IG Lead and DPO holds the casting vote in any decision, then his vote will be discounted.

Step 1: Identify the Need for a DPIA

As above

Step 2: Describe the Processing

This is clearly detailed in the ICO's guidance, reproduced verbatim:

The nature of the processing is what you plan to do with the personal data. This should include, for example:

- How you collect the data
- How you store the data
- How you use the data
- Who has access to the data
- Who you share the data with
- Whether you use any processors
- Retention periods
- Security measures
- Whether you are using any new technologies
- Whether you are using any novel types of processing

- Which screening criteria you flagged as likely high risk.

The scope of the processing is what the processing covers. This should include, for example:

- The nature of the personal data
- The volume and variety of the personal data
- The sensitivity of the personal data
- The extent and frequency of the processing
- The duration of the processing
- The number of Data Subjects involved
- The geographical area covered.

The context of the processing is the wider picture, including internal and external factors that might affect expectations or impact. This might include, for example:

- The source of the data
- The nature of your relationship with the individuals
- The extent to which individuals have control over their data
- The extent to which individuals are likely to expect the processing
- Whether they include children or other vulnerable people
- Any previous experience of this type of processing
- Any relevant advances in technology or security
- Any current issues of public concern
- In due course, whether you comply with any GDPR codes of conduct (once any have been approved under Article 40) or GDPR certification schemes
- Whether you have considered and complied with relevant codes of practice.

The purpose of the processing is the reason why you want to process the personal data. This should include:

- Your legitimate interests, where relevant
- The intended outcome for individuals, and
- The expected benefits for you or for society as a whole.

Steps 3 & 4: Consider Consultation

We should seek the views of individuals, or their representatives, unless there is a good reason not to. If our DPIA decision is at odds with the views of individuals, we will document our reasons for disregarding their views. If we decide that it is not appropriate to consult individuals, we will record this decision as part of our DPIA with a clear explanation. If we use a Data Processor, we may need to ask them for information and assistance; our contracts with processors require them to assist. We should consult all relevant internal stakeholders, in particular anyone with responsibility for information security.

Step 5: How Do We Assess Necessity and Proportionality?

We should consider:

- Do our plans help to achieve our purpose?
- Is there any other reasonable way to achieve the same result?

The Article 29 guidelines also say we should include how we ensure data protection compliance, which are a good measure of necessity and proportionality. In particular, we should include relevant details of:

- Our lawful basis for the processing
- How we will prevent function creep
- How we intend to ensure data quality

- How we intend to ensure data minimisation
- How we intend to provide privacy information to individuals
- How we implement and support individuals rights
- Measures to ensure our processors comply
- Safeguards for any international transfers.

Step 6: How Do We Identify and Assess Risks?

We should consider the potential impact on individuals and any harm or damage that might be caused by our processing – whether physical, emotional or material. In particular we will look at whether the processing could possibly contribute to:

- Inability to exercise rights (including but not limited to privacy rights)
- Inability to access services or opportunities
- Loss of control over the use of personal data
- Discrimination
- Identity theft or fraud
- Financial loss
- Reputational damage
- Physical harm
- Loss of confidentiality
- Re-identification of pseudonymised data, or
- Any other significant economic or social disadvantage.

The impact on society as a whole may also be a relevant risk factor. For example, it may be a significant risk if our intended processing leads to a loss of public trust. We should include an assessment of the security risks, including sources of risk and the potential impact of each type of breach – including illegitimate access to, modification of or loss of personal data. We must make an 'objective assessment' of the risks. Using a structured matrix to think about likelihood and severity of risks will be useful:

Severity of impact				
	Serious harm	**Low risk**	**High risk**	**High risk**
	Some impact	**Low risk**	**Medium risk**	**High risk**
	Minimal impact	**Low risk**	**Low risk**	**Low risk**
		Remote	Reasonable possibility	More likely than not
		Likelihood of harm		

Step 7: How Do We Identify Mitigating Measures?

Against each risk identified, we will record the source of that risk. We should then consider options for reducing that risk. For example:

- Deciding not to collect certain types of data
- Reducing the scope of the processing

- Reducing retention periods
- Taking additional technological security measures
- Training staff to ensure risks are anticipated and managed
- Anonymising or pseudonymising data where possible
- Writing internal guidance or processes to avoid risks
- Using a different technology
- Putting clear data sharing agreements into place
- Making changes to privacy notices
- Offering individuals the chance to opt out where appropriate
- Implementing new systems to help individuals to exercise their rights.

We should record whether the measure would reduce or eliminate the risk. We can take into account the costs and benefits of each measure when deciding whether or not they are appropriate.

Step 8: How Do We Conclude Our DPIA?

We should then record:

- What additional measures we plan to take
- Whether each risk has been eliminated, reduced, or accepted
- The overall level of 'residual risk' after taking additional measures
- Whether we need to consult the ICO.

The Corner Surgery will publish our formal DPIAs to aid transparency and accountability, and engender trust and confidence in the ways that we process patients' data. We will need to keep any DPIA under review, and may need to repeat it if there is a substantial change to the nature, scope, context or purposes of our processing.

When Do We Need to Consult the ICO?

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

If we have carried out a DPIA that identifies a high risk, with processing on a large scale, and we cannot take any measures to reduce this risk, we need to consult the ICO. We cannot go ahead with the processing until we have consulted the ICO & they have responded. Please note, The Corner Surgery is a small practice, with ~4000 Data Subjects and ~15 staff, so most processing will not be on a large scale.

We will refer the DPIA to the ICO if processing data would, or *could*:

- Put the practice at risk of breaching the common law duty of confidentiality
- Put the practice at risk of breaching one or more of the data protection principles (Article 5)
- Put the practice at risk of breaching one or more of the GDPR Articles
- Deny (or impact significantly) data subjects rights, such as their right to be informed, to rectification, to restrict processing or to erasure.

The focus is on the 'residual risk' *after* any mitigating measures have been taken. If our DPIA identified a high risk but we have taken measures to reduce this risk so that it is no longer a high risk, then we do not need to consult the ICO.

Dr David Smith